Risk analysis in information systems: A fuzzification of the MAGERIT methodology ☆

E. Vicente *, A. Mateos, A. Jiménez-Martín

Decision Analysis and Statistics Group, Departamento de Inteligencia Artificial, Universidad Politécnica de Madrid, Campus de Montegancedo S/N, Boadilla del Monte, 28660 Madrid, Spain

A B S T R A C T

Several methodologies based on ISO/IEC 27000 international standard have been developed to deal with risk analysis in information systems (IS). These methodologies do not, however, consider imprecise val-uations, but use precise values on different, usually percentage, scales.

We propose an extension of the MAGERIT methodology based on classical fuzzy computational models. A linguistic term scale is used to represent asset values, their dependencies and frequency and asset deg-radation associated with threats. Computations are based on trapezoidal fuzzy numbers associated with linguistic terms. A similarity function is used to associate a linguistic term on the previously defined scale to the trapezoidal fuzzy numbers resulting from computations. Finally, regarding the selection of preven-tive safeguards to reduce risks in IS, we propose a dynamic programming-based method that incorpo-rates simulated annealing to tackle optimizations problems with the aim of minimizing costs while keeping the risk at acceptable levels.

An example of an administrative unit using in-house and third-party information systems internally and to provide public information services is used to illustrate the methodology.

1. Introduction

Information systems (IS) are composed of a set of data management elements designed to provide services and benefits in areas as far a part as public administration, industrial control, banking or geographical and weather information.

Technological developments and universal internet access have led to an increase in system vulnerabilities, since organizations have connected ISs to corporate and even public networks to which non-authorized personnel could have access unless appropriate action is taken. Besides, people within the organization have to be trained in and aware of IS support technology, as technology misuse can cause disastrous failures.

On top of these vulnerabilities caused by recent technological developments, there are other traditional issues, such as integrity facilities or the custody of not necessarily digital documents, on which new technologies have also had an impact. Therefore, ISs have to be analysed with a view to risk minimization by means of well-planned actions to protect information, processes and services from possible threats. Threats range from acts of terrorism, industrial espionage, etc. to a simple unintentional human error by an operator.

International standards establishing requirements for the certification of *security information management systems* (SIMS) originated in the BS 7799 security standard, proposed by the British Standards Institution (BSI). The first part of the standard (BS 7799-1), published in 1995, provided for the first time a set of best practices for managing the security of information to be used by any company or organization, whereas the second part (BS 7799-2) sets out SIMS requirements for certification by independent auditors.

In 1999, the ISO/IEC JTC 1 committee accepted the BS 7799-1 without major changes as ISO/IEC 17799, which was renumbered as ISO/IEC 27002 in 2005, whereas BS 7799-2 was adopted as ISO/IEC 27001. This is the fundamental rule of all ISO/IEC 27000 standards, which in the number ranges 27,000–27,019 and 27,030–27,044 provide the security information management framework that underpins national or corporate adaptations, and different risk analysis and management methodologies for IS, respectively. Currently, both the ISO/IEC 27001 and ISO IEC

☆ The paper was supported by Madrid Regional Government Project S-2009/ESP-1685 and the Spanish Ministry of Science and Innovation Project MYTM2011-28983-C03-03

* Corresponding author. Tel.: +34 91 336 6596; fax: +34 91 352 4819.

E-mail addresses: e.vicentecestero@upm.es (E. Vicente), amateos@fi.upm.es (A. Mateos), antonio.jimenez@upm.es (A. Jiménez-Martín).

27002 are under review, and a new versions are expected to be published in 2013.

Quality management systems have traditionally used the *plan-do-check-act* cycle or *continuous improvement model*, which many international methodologies based on the ISO/IEC 27000 series have also tended to adopt. This model establishes a system of indicators and metrics that are comparable over time to quantify the organizational improvement progress and suggests a three-stage risk analysis and management methodology, see Fig. 1.

The *planning stage* establishes the necessary points for starting up the project, defines objectives, and identifies participants and competencies. Risk analysis is the central part of SIMS and is included in the *plan* phase of the continuous improvement model. The purpose of risk identification is to determine the potential losses (impacts) that could occur in the organization if the threats to the IS components materialize, identifying such components (assets), as well as their relations (dependencies), the potential threats and their frequency and asset degradation levels. Finally, the *risk management stage* determines the safeguards and strategies that reduce impact and risk.

The ISO/IEC 27000 [12,13] stipulations are adapted by each country leading to different methodologies, such as MAGERIT [16] (Ministerio de Administraciones Públicas, Spain), MEHARI [17] (Club de la Securit de l'Information Francais, France), CRAMM [8] (Central Computing and Telecommunications Agency, UK), OCTAVE and OCTAVE-S [1] (Carnegie Mellon University, USA) or NIST 800-30 [21] (National Institute of Standards and Technology, USA).

In Spain, the Consejo Superior de Administración Electrónica (Council for Electronic Administration) established the MAGERIT methodology (Methodology Analysis and Risk Management Information Systems) with the aim of deploying a common framework for risk analysis and management in IS on the basis of ISO/IEC 27000 standards. This methodology includes the following milestones:

1. *Identification and valuation of assets*
   An asset is anything that is of value to the organization and therefore requires protection. A few data, information or business process assets often account for a total value of an organization's assets. These assets are called *terminal assets* . Other assets (*support assets* such as hardware, software, personnel, and facilities) are valuable insofar as they are beneficial to the terminal assets, and they inherit the terminal asset value, according to the resulting benefit. Thus, support assets have no intrinsic value; they take their value from terminal assets.
   The identified assets of the organization are then valued. Some assets may have a monetary value (how much money the organization would lose if this asset stopped working), whereas others require a qualitative assessment (if an asset stops working the losses would be very high, low, medium, etc.).

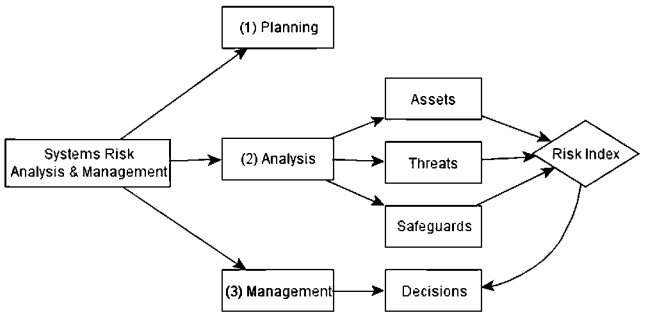

Fig. 1. Risk analysis and management in information systems.

   As mentioned above, the support assets inherit their values from terminal assets depending on how they influence each other. So, we have to determine the dependency relationships of the terminal assets with respect to support assets, and also dependency relationships between support assets.
2. *Threat identification*
   A *threat* is an event that can trigger an incident in the organization, causing damage or intangible material loss to assets. A threat may be of natural or human, accidental or deliberate origin. Some threats can affect more than one asset. In such cases, threats can cause different impacts depending on what assets are affected. A detailed list of threats is available in Annex C of ISO IEC 27005. MAGERIT suggests two threat assessment measures: *degradation*, the damage that the threat can cause to the asset, and *frequency*, how often the threat materializes.
3. *Identification and valuation of impact and risk indicators*
   It is then necessary to qualitatively identify the consequences and establish impact and risk indicators for the valued assets and threats. The impact of a threat on an asset is the product of the asset value multiplied by the respective degradation. Risk is the product of the impact of the threat multiplied by the respective frequency.
4. *Selection of safeguards*
   Safeguards are measures for addressing threats. They can be procedures, personnel policies, technical solutions or physical security measures at the facilities. These safeguards can be *preventive*, if they reduce the frequency of threats; or *palliative*, if they reduce the degradation of assets caused by threats [16].

The MAGERIT methodology provides two computational models: a quantitative model and an ordinal symbolic (qualitative) model. The quantitative model states precise values within the range [0,1] in order to measure magnitudes, whereas the qualitative model establishes an ordinal scale. In neither case is vague or imprecise information about the input parameters allowed. In our opinion, this is an important drawback of the methodology. Moreover, additional advantages could be gained using a classical fuzzy linguistic computational rather than the ordinal symbolic computational model provided by MAGERIT.

In this paper, we propose an extension of the methodology proposed by Vicente et al. [24], to adapt the MAGERIT methodology for risk analysis in IS to account for vague or imprecise information about the input parameters on the basis of classical fuzzy linguistic computational models. A fuzzy linguistic term scale is constructed to valuate the different risk analysis elements, the arithmetic proposed by Xu et al. [32] based on trapezoidal fuzzy numbers is used to make computations and, finally, a similarity function is used to translate the resulting trapezoidal fuzzy numbers into a linguistic term on the previously defined scale.

In Section 2, we briefly introduce fuzzy computational models and describe the computational models included in the MAGERIT methodology and its drawbacks. Consequently, we have decided to extend the MAGERIT computational model to solve these problems. Section 3 introduces the fuzzy extension of the MAGERIT methodology. First, we review some operations on trapezoidal fuzzy numbers and introduce a fuzzy evaluation of asset dependencies. Second, we provide a fuzzy five-component valuation of assets. Threats and asset risk impact indicators are then described. Then, we introduce the similarity function used to associate a linguistic term from the previously defined set with the resulting trapezoidal fuzzy numbers. Finally, we tackle the selection of preventive safeguards to address threats. The methodology is illustrated in Section 4 using an example concerning an administration unit that uses its in-house and third-party ISs for internal operations and to provide public information services. Finally, some conclusions and future research are discussed in Section 5.

2. Fuzzy computational models and the MAGERIT methodology

Fuzzy logic introduced by Zadeh in 1965 [33] is a mathematical tool for modeling concepts using vague or imprecise measurements. This tool is especially interesting in computational models where experts are unable to give specific values to certain variables. Instead, it assigns linguistic terms of a previously defined scale from a total order.

For example, $\mathcal{L} = \{l_0 \approx VeryLow, l_1 \approx Low, l_2 \approx Medium, l_3 \approx High, l_4 \approx VeryHigh\}$ is a five-term linguistic scale in which we can imprecisely measure a given magnitude. The linguistic term scale must satisfy the following properties [10]:

1. There is a negation operator $Neg(l_i) = l_j$ such that $j = n - i$, where n is the cardinality of the linguistic scale.
2. There exists a total order $l_i \leqslant l_j \iff i \leqslant j$.

These linguistic terms can be represented by functions $\mu : \Re \to [0,1]$ to indicate the degree of membership of the value $x \in \Re$ to the corresponding linguistic term. This membership function is usually triangular, trapezoidal or Gaussian. For example, a normalized trapezoidal fuzzy number, which can be denoted by $\widetilde{A} = (a_1, a_2, a_3, a_4)$, has a membership function (see Fig. 2)

$$\mu_{\widetilde{A}}(x) = \begin{cases} \frac{x-a_1}{a_2-a_1} & if\ a_1 \leqslant x \leqslant a_2 \\ 1 & if\ a_2 \leqslant x \leqslant a_3 \\ \frac{x-a_4}{a_3-a_4} & if\ a_3 \leqslant x \leqslant a_4 \\ 0 & otherwise \end{cases}. \tag{1}$$

Two linguistic computational models can be used within fuzzy logic:

1. The *classical linguistic computational model* defines a fuzzy number arithmetic using operations with membership functions, as an extension of real arithmetic. These arithmetic operations on fuzzy numbers result in a new fuzzy number, which generally does not necessarily belong to the previously defined linguistic scale. Then, similarity measures of fuzzy numbers are used to decide which element on the scale is associated with the result of these operations. For examples of the classical linguistic computational model, see [31,4,6,27].
2. *Ordinal symbolic computational models* do not use membership functions, but identifies the given scale with an interval of length $n-1$, where n is the cardinality of the linguistic scale, and make computations between linguistic terms whose results are real numbers in the associated interval:

   $$\varphi : \{l_0, \ldots, l_{n-1}\} \hookrightarrow [0, n-1], \quad l_i \mapsto \varphi(l_i) = i.$$

   For example, $\{l_0, \ldots, l_4\} \approx [0,4] \subset \Re$. Commonly used operators are the convex combination [10] (like the arithmetic or weighted average), minimum, maximum or the *ordered weighted aggregation* (OWA), among others. As in the classical model, the real results of the operators may not belong to the linguistic scale, but one of the linguistic terms is associated with the result using an approximation function.

   The *2-tuple model* [10] is an ordinal symbolic computational model designed to resolve the problem of discretizing the operation space on the linguistic term scale. The results of symbolic operations performed on the scale $\mathcal{L} = \{l_0, \ldots, l_{n-1}\} \approx [0, n-1]$ are given by tuple (l_i, α), where l_i is the linguistic term closest to the result and $\alpha \in [-0.5, 0.5)$ represents the distance to the term. For example, if an operation on the symbolic scale $\{l_0, \ldots, l_4\}$ outputs the value 3.25, then that value is the tuple $(l_3, 0.25)$.

   Then, we obtain the function

   $$\Delta : [0, n-1] \to \mathcal{L} \times [-0.5, 0.5), \quad \beta \mapsto \Delta(\beta) = (l_i, \alpha),$$

   with $i = round(\beta)$, the rounding operator, and $\alpha = \beta - i$.

   It is verified that Δ is bijective, and its inverse is $\Delta^{-1}(l_i, \alpha) = i + \alpha$. This guarantees the preservation of information, however the 2-tuple method does not allow non-linear operators. Three linear operators are introduced in [10]: the arithmetic mean, the weighted average and the OWA operator, but it is not possible to multiply two linguistic terms in the 2-tuple symbolic model. The virtual language model [31] or the 2-tuples proportional model [27] propose other operators for the 2-tuple model, but they do not include the product of linguistic terms.

   Different applications of the *2-tuple model* have been reported in the literature, such as [19] for multi-attribute decision-making under risk, [20] for security evaluation in computer networks, [20] in the educational field, [26] in market research or [2] in data mining. Two applications of the *2-tuple model* to group decision-making can be found in [29,30].

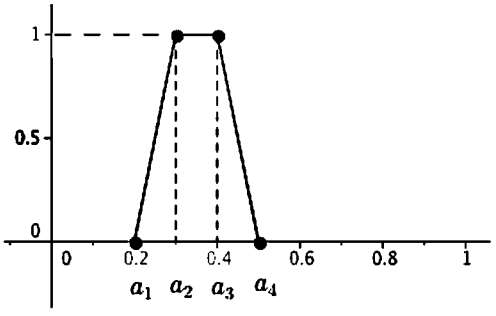

Fig. 2. Membership function.

There is a loss of information in both the classical and the symbolic models as a result of the approach to be performed either by the similarity function in the classical model or by using the approximation function in the symbolic model.

The MAGERIT methodology provides two computational models: a quantitative model and an ordinal symbolic (qualitative) model.

Quantitative model. This model directly measures each magnitude in the range $[0,1]$ so that the minimum value corresponds to zero and the maximum to one. The main drawback of this model is that experts may find it difficult to assign precise values to the input parameters of the model, and the results are sensitive to these values.

Qualitative model. The ordinal symbolic model establishes an ordinal scale

$$V = \{v_0, \ldots, v_{n-1}\} \overset{\varphi}{\approx} [0, n-1].$$

The different risk magnitudes are measured on this scale, where v_0 is a term under which the magnitude is considered negligible. The operators considered in this qualitative model are:

1. *max* and *min* operators.
2. *product by scalars in* $[0,1]$, which can represent magnitudes such as the degradation associated with the materialization of a threat on an asset or the potential reduction of the impact of the threat thanks to a safeguard. For example, if a certain safeguard reduces impact v_i by $\alpha\%$, then this impact is reduced to a level
   $\beta = v_i \times (1 - \frac{\alpha}{100}) \overset{\varphi}{\approx} \varphi(v_i) \times (1 - \frac{\alpha}{100}) = i \times (1 - \frac{\alpha}{100}) \in [0, n-1]$.

As mentioned above, the result will not necessarily be a linguistic term on the given scale. In the MAGERIT methodology, a linguistic scale term is assigned to the result of these operators by rounding. This is computed in the example above as

$\phi : [0, n-1] \to \{v_0, \ldots, v_{n-1}\}$,

$$\phi(\beta) = round(\beta) = round\left(i \times \left(1 - \frac{\alpha}{100}\right)\right) \in [0, n-1] \cap \mathbb{N} = \{v_0, \ldots, v_{n-1}\}.$$

For example, using the scale $v_0, \ldots, v_4$, let us assume that a threat implies an impact value v_3 on an information asset and that the frequency of the threat is 0.4. Then, MAGERIT computes the risk associated with this threat on the asset as $0.4 \times v_3 \overset{\varphi}{\approx} 0.4 \times \varphi(v_3) = 0.4 \times 3 = 1.2$ and $\phi(1.2) = v_1$.

This computational model has several drawbacks:

1. Some magnitudes, such as the degradation or the frequency of a threat, have to be assessed by means of precise percentages. Some operations, such as the product or the sum of linguistic terms, whose results may be outside the interval $[0, n-1]$, are prohibited. This may have unrealistic consequences for risk analysis. For example, if a threat has a very high impact, v_4, and a frequency of 0.5, then the risk implied by this threat is v_2 (medium), but, with this impact and frequency a risk is perceived to be very high.
   The problem is that a probability 0.5 is perceived as high in many real-life activities, particularly for activities that appear to be most important and have a major impact on our lives. Thus, it is not advisable to use the product by probabilities viewed as real numbers [0,1], as MAGERIT does.
2. A lot of information is lost through the rounding. Note that the function φ is not bijective.
3. Terms such as $0.5 \times v_3 = 1.5$ are somewhat ambiguous. We do not know whether this value should be assigned to v_1 or v_2.
4. It does not take advantage of the properties associated with the membership function used in the classical model.
5. It needs symmetric and uniformly distributed linguistic terms scales.

Consequently, we have decided to extend the MAGERIT computational model from the classical linguistic fuzzy model perspective since it seems the better choice because it enables to model magnitudes using vague or imprecise measurements and because of the properties associated with the use of membership functions as well as because of drawbacks associated with ordinal symbolic computational models

Note that classical linguistic fuzzy models also result in a loss of information caused by the procedure enacted by the similarity function. However, the similarity function will not be applied until the end of the risk analysis of the IS, when a linguistic term is associated with the derived risk or impact fuzzy value, if required by the experts. In other words, unlike the ordinal symbolic model provided by MAGERIT, where the rounding operation is performed after each computation, the trapezoidal fuzzy numbers output in the different computations (indirect dependences, etc.) will be propagated throughout the risk analysis stages in the risk analysis that we propose. Moreover, the similarity function is not used to select preventive safeguards. This constitutes a minor loss of information and, consequently, another advantage of the fuzzy extension that we propose.

3. Fuzzy extension of MAGERIT methodology

Let us consider the set of normalized trapezoidal fuzzy numbers with support in $[0,1]$, $TF[0,1]$, i.e. $\widetilde{A} = (a,b,c,d)$, with $0 \leqslant a \leqslant b \leqslant c \leqslant d \leqslant 1$, together with a membership function $\mu_{\widetilde{A}}(x)$, see (1) and Fig. 2.

We use the following arithmetic proposed in [32] in $TF[0,1]$: If $\widetilde{A}_1 = (a_1, b_1, c_1, d_1)$ and $\widetilde{A}_2 = (a_2, b_2, c_2, d_2)$, then

$$\widetilde{A}_1 \oplus \widetilde{A}_2 = (a_1 + a_2 - a_1a_2, b_1 + b_2 - b_1b_2, c_1 + c_2 - c_1c_2, d_1 + d_2 - d_1d_2),$$
$$\widetilde{A}_1 \otimes \widetilde{A}_2 = (a_1a_2, b_1b_2, c_1c_2, d_1d_2).$$

Both operations ($\oplus$ and $\otimes$) are well defined. $\oplus$ and $\otimes$ are two internal composition laws in $TF[0,1]$ that verify commutative and associative properties and have a neutral element.

3.1. Fuzzy valuation of dependencies

As cited in the introduction, the assets in IS are connected by dependency relationships, and a failure of one asset may affect other assets, forming an acyclic graph, as shown in Fig. 3.

Asset A_j *depends* on the asset A_i (or A_i *influences* A_j), denoted by (A_i, A_j) (graphically $A_i \to A_j$), if a failure in asset A_i causes a failure in the asset A_j with any given probability. This probability is usually referred to as the *degree of dependency* of A_j with respect to A_i or the *influence* of A_i over A_j, which we denote by $dd(A_i, A_j)$.

Proposed IS risk analysis methodologies assign just a percentage to indicate the degree of dependency between two assets, and sometimes even propose the use of a Boolean value indicating whether or not this dependency exists regardless of the degree of dependency, see [16,17,8,1,21]. We propose the use of trapezoidal fuzzy numbers to represent these dependencies. Consequently, $\widetilde{dd}(A_i, A_j) \in TF[0,1]$ and the experts can build a linguistic term set to intuitively define the dependency between two assets under uncertainty.

The dependency between assets in the dependency structure need not be direct but can be transitive. Namely, if (A_i, A_j) and (A_j, A_k), then (A_i, A_k).

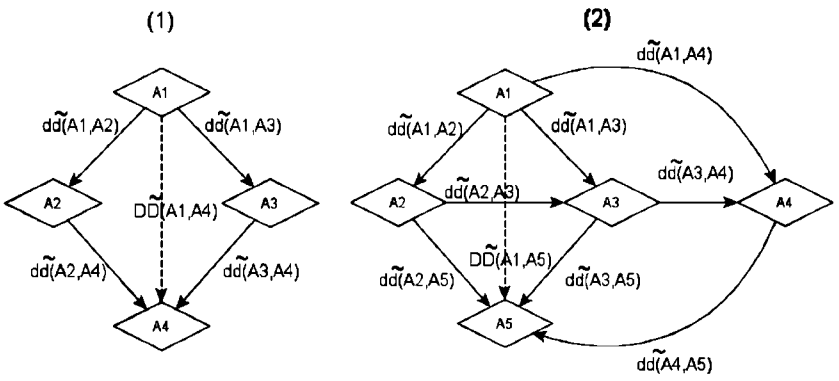

Fig. 3. Asset dependencies structure in information systems.

Our aim then is to compute the indirect asset dependencies since assets values are accumulated from terminal assets through these dependencies.

The degree of dependency of asset A_k with respect to A_i, $\widetilde{DD}(A_i,A_k)$, is computed as follows.[1] We denote by $\mathbf{P}=\{P_1,\ldots,P_s\}$ the set of paths in the analysis of the influence of A_i over A_k. These paths are a sequence of consecutive arcs in the acyclic graph connecting the corresponding vertices A_i and A_k. Then,

(A) If all assets (excluding A_i and A_k) in the paths in $\mathbf{P}$ are influenced by only one asset, then

$$\widetilde{DD}(A_i,A_k)=\overset{s}{\underset{j=1}{\oplus}}\widetilde{DD}(A_i,A_k|P_j),$$

where $\widetilde{DD}(A_i,A_k|P_j)=\widetilde{dd}(A_i,A_{j1})\otimes\widetilde{dd}(A_{j1},A_{j2})\otimes\ldots\otimes\widetilde{dd}(A_{jn},A_k)$, where $P_j:(A_i\to A_{j1}\to A_{j2}\to\ldots\to A_{jn}\to A_k)$.

(B) Otherwise, we assume that the first r paths in $\mathbf{P}$ are formed by assets (excluding A_i and A_k) influenced by only one asset, and the remaining $s-r$ paths include at least one asset influenced by two or more assets. Then, for the r first paths, we proceed as in A), and we denote by $\mathbf{S}$ the set including the $s-r$ remaining paths. We proceed with $\mathbf{S}$ as follows:

(i) Compute the set of non-terminal assets in $\mathbf{S}$ influenced by two or more assets, denoted by I, and the subset of I including assets uninfluenced by any other asset in I, denoted by NI.

(ii) We consider an asset A_r in NI. Then, we simplify the paths in $\mathbf{S}$ that include asset A_r making $A_i\to A_r\to\ldots\to A_k$, with $\widetilde{dd}(A_i,A_r)=\widetilde{DD}(A_i,A_r)$ (computed as in A)).

(iii) Remove repeated paths from $\mathbf{S}$ and keep only one instance.

(iv) Build I and NI again from $\mathbf{S}$.

(v) If NI is not empty, go to (ii). Otherwise, the algorithm finishes.

Let us denote the resulting set of paths by $\mathbf{S}=\{P'_1,\ldots,P'_m\}$, with $m\leqslant s-r$. Then, the degree of dependency of A_k regarding A_i is

$$\widetilde{DD}(A_i,A_k)=\overset{r}{\underset{j=1}{\oplus}}\widetilde{DD}(A_i,A_k|P_j)\overset{m}{\underset{l=1}{\oplus}}\widetilde{DD}(A_i,A_k|P'_l).$$

Fig. 3 shows two examples of possible dependency structures in IS. In the first example, $P=\{P_1:(A_1\to A_2\to A_4),P_2:(A_1\to A_3\to A_4)\}$, all the assets (excluding A_1 and A_4) are influenced by one asset. Then, we apply A) again leading to

$$\begin{aligned}\widetilde{DD}(A_1,A_4)&=\widetilde{DD}(A_1,A_4|P_1)\oplus\widetilde{DD}(A_1,A_4|P_2)\\&=[\widetilde{dd}(A_1,A_2)\otimes\widetilde{dd}(A_2,A_4)]\oplus[\widetilde{dd}(A_1,A_3)\otimes\widetilde{dd}(A_3,A_4)].\end{aligned}$$

In the second example,

$$\begin{aligned}\mathbf{P}=\{&P_1:(A_1\to A_2\to A_5),P_2:(A_1\to A_2\to A_3\to A_5),\\&P_3:(A_1\to A_2\to A_3\to A_4\to A_5),P_4:(A_1\to A_3\to A_5),\\&P_5:(A_1\to A_3\to A_4\to A_5),P_6:(A_1\to A_4\to A_5)\},\end{aligned}$$

asset A_3 is influenced by A_1 and A_2, and A_4 is influenced by A_1 and A_3. Therefore, we apply B) with $r=1$ and $\mathbf{S}=\{P_2,P_3,P_4,P_5,P_6\}$ and proceed as follows:

(i) $I=\{A_3,A_4\}$ and $NI=\{A_3\}$.

(ii) We select A_3, then we simplify the paths P_2, P_3, P_4 and P_5 to $P'_2:(A_1\to A_3\to A_5)$, $P'_3:(A_1\to A_3\to A_4\to A_5)$, $P'_4:(A_1\to A_3\to A_5)$ and $P'_5:(A_1\to A_3\to A_4\to A_5)$, respectively, with $\widetilde{dd}(A_1,A_3)=\widetilde{DD}(A_1,A_3)=(\widetilde{dd}(A_1,A_2)\otimes\widetilde{dd}(A_2,A_3))\oplus\widetilde{dd}(A_1,A_3)$.

(iii) $\mathbf{S}=\{P'_2,P'_3,P_6\}$ since $P'_2=P'_4$ and $P'_3=P'_5$.

(iv) $I=\{A_4\}$ and $NI=\{A_4\}$.

(v) Go to (ii).

(ii) We select A_4, then we simplify the paths P'_3 and P_6 to $P''_3:(A_1\to A_4\to A_5)$, and $P'_6:(A_1\to A_4\to A_5)$, respectively, with $\widetilde{dd}(A_1,A_4)=\widetilde{DD}(A_1,A_4)=(\widetilde{dd}(A_1,A_3)\otimes\widetilde{dd}(A_3,A_4))\oplus\widetilde{dd}(A_1,A_4)$.

(iii) $\mathbf{S}=\{P'_2,P''_3\}$ since $P''_3\equiv P'_6$.

(iv) $I=empty$ and $NI=empty$.

(v) The algorithm finishes since $NI=empty$.

Finally, $\mathbf{S}=\{P'_2,P''_3\}$ and the degree of dependency of A_5 regarding A_1 is

$$\begin{aligned}\widetilde{DD}(A_1,A_5)&=\widetilde{DD}(A_1,A_5|P_1)\oplus\widetilde{DD}(A_1,A_5|P'_2)\oplus\widetilde{DD}(A_1,A_5|P''_3)\\&=\left(\widetilde{dd}(A_1,A_2)\otimes\widetilde{dd}(A_2,A_5)\right)\\&\quad\oplus\left(\widetilde{dd}(A_1,A_3)\otimes\widetilde{dd}(A_3,A_5)\right)\\&\quad\oplus\left(\widetilde{dd}(A_1,A_4)\otimes\widetilde{dd}(A_4,A_5)\right).\end{aligned}$$

Note that transactions between trapezoidal fuzzy numbers representing linguistic terms from a set in $[0,1]$ will remain in $TF[0,1]$, and the results of these operations can be translated into one of the linguistic terms of the set by means of a similarity function. Furthermore, the operation $\oplus$ is consistent with the methodologies established for risk analysis and management in IS, allowing performances in probabilistic terms.

Let us consider these issues in more detail. The MAGERIT [16] methodology uses crisp probabilities to determine the dependency, as mentioned before, and proposes the following operation: $a\bar{\oplus}b=a+b-ab$.

Operation $\bar{\oplus}$ is a special case of the operation proposed in [32] and used in this paper, $\oplus$, since a crisp probability $a\in[0,1]$ can be written as the trapezoidal fuzzy number

$$\begin{aligned}\tilde{a}\oplus\tilde{b}&=(a,a,a,a)\oplus(b,b,b,b)\\&=(a+b-ab,a+b-ab,a+b-ab,a+b-ab)=\widetilde{a\bar{\oplus}b}\\&\approx a\bar{\oplus}b.\end{aligned}$$

Operation $\otimes$ extends naturally to the product of real numbers.

Therefore, by defining operations $\oplus$ and $\otimes$, we have successfully extended the basic operations using IS risk analysis and management methodologies to the context of fuzzy numbers.

As an example, let us consider the first dependency structure in Fig. 3 and the linguistic term set in Table 1 and Fig. 4. Note that other linguistic terms scales could be used, with a different number of terms or with different membership functions (triangular, non-symmetrical, etc.) instead of the trapezoidal. A solution for possible conflicts in the valuations in a group decision-making context is an interesting future research line. Moreover, if the expert is not confident with a predetermined scale, he/she could also use a method for extracting a fuzzy number representing a probabilistic

Table 1
Fuzzy linguistic term set.

Term	Fuzzy number
Very low (VL)	(0,0,0,0.05)
Low (L)	(0,0.05,0.15,0.25)
Medium–low (M–L)	(0.15,0.25,0.35,0.45)
Medium (M)	(0.35,0.45,0.55,0.65)
Medium–high (M–H)	(0.55,0.65,0.75,0.85)
High (H)	(0.75,0.85,0.95,1)
Very high (VH)	(0.95,1,1,1)

[1] To avoid ambiguity (see Fig. 3), we will write "DD" to refer to total dependency between two assets separated by other intermediate assets, and "dd" when they are directly connected.

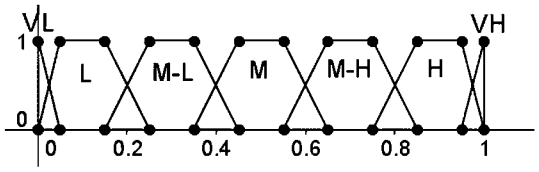

Fig. 4. A seven-member linguistic term set.

judgment for each event, such as the one based on bettings and lotteries proposed in [25], which accounts for a group context, because individual conflicting views or judgments can be captured through imprecise responses.

On the other hand, experts have assigned the influences shown in Table 2. Then, the degree of dependency of A_1 with respect to A_4 is

$$\widetilde{DD}(A_1,A_4) = \left[\widetilde{dd}(A_1,A_2) \otimes \widetilde{dd}(A_2,A_4)\right] \oplus \left[\widetilde{dd}(A_1,A_3) \otimes \widetilde{dd}(A_3,A_4)\right] = [H \otimes M] \oplus [M{-}H \otimes M] = (0.404, 0.563, 0.719, 0.843).$$

3.2. Fuzzy valuation of assets

MAGERIT defines the *value of an asset* as the losses that would be sustained if the respective asset is no longer available. These can be losses of money, user confidence, the organizational prestige, etc. Assets are usually evaluated taking into account the following five components [16]:

- *Confidentiality*. How much damage would it cause if the asset is disclosed to someone it should not be? This is a typical data inspection.
- *Integrity*. How much damage would it cause if the asset is damaged or corrupt? This is a typical data inspection. Data can be manipulated, be wholly or partially false, or even missing.
- *Authenticity*. How much damage would it cause if we do not exactly know who has done what? This is a typical services (user authentication) and data (authenticity of the person accessing data to write or read) inspection.
- *Traceability*. How much damage would it cause if it is not known for whom the service is being provided?, i.e. who does what and when? How much damage would it cause if it is not known who accessed what data and what they did with them?
- *Availability*. How much damage would it cause if the asset is not available or cannot be used? This is a typical services inspection.

Only the terminal assets have an associated value for the above components. The other assets accumulate value from terminal assets on the basis of dependency relationships. We again use the set of linguistic terms that represent trapezoidal fuzzy numbers to represent uncertainty when valuating the terminal assets.

Let us denote assets by $\widetilde{v}_j = (\widetilde{v}_{j_{(1)}}, \widetilde{v}_{j_{(2)}}, \widetilde{v}_{j_{(3)}}, \widetilde{v}_{j_{(4)}}, \widetilde{v}_{j_{(5)}})$, where $\widetilde{v}_{j_{(i)}}$ is a linguistic term assigned by an expert for the ith value component in asset A_j. If we denote by *TAS* the terminal asset set, then the value of asset A_j with respect to terminal assets is:

Table 2
Fuzzy degrees of dependency.

Influence	Term	Fuzzy number
$A1 \rightarrow A2$	High	(0.75,0.85,0.95,1)
$A2 \rightarrow A4$	Medium	(0.35,0.45,0.55,0.65)
$A1 \rightarrow A3$	Medium-High	(0.55,0.65,0.75,0.85)
$A3 \rightarrow A4$	Medium	(0.35,0.45,0.55,0.65)

$$\widetilde{v}_{j_{(i)}} = \sum_{A_k in TAS} (\widetilde{DD}(A_j,A_k) \otimes \widetilde{v}_{k_{(i)}}). \quad (2)$$

Note that the sums in the above expression are computed as follows: $\widetilde{A}_1 + \widetilde{A}_2 = (a_1 + a_2, b_1 + b_2, c_1 + c_2, d_1 + d_2)$.

3.3. Threats

A *threat* is an event that can trigger an incident in our organization, causing damage or intangible material loss to the assets, and an *attack* is any deliberate action aimed at violating the IS security mechanisms.

Once assets have been valuated, the next step in the risk analysis methodology is to assess threats and estimate indicators of the impact on and risk to assets. MAGERIT suggests two threat assessment measures: *degradation*, the damage that the threat can cause to the asset; and *frequency*, how often the threat materializes.

We will again use fuzzy linguistic terms rather than percentages and probabilities to represent degradation and frequency. A threat is a vector $\vec{\widetilde{T}} = (\widetilde{D}, \widetilde{f})$ whose components are degradation and frequency. A degradation has to be established for each of the five asset components described in the Section 3.

Let us consider a threat on asset A_j whose degradation in each component is given by the vector

$$\vec{\widetilde{D}} = (\widetilde{d}_1, \widetilde{d}_2, \widetilde{d}_3, \widetilde{d}_4, \widetilde{d}_5),$$

i.e., the threat T causes a degradation $\widetilde{d}_i$ in the ith component of the asset.

When the threat is realized, each component is affected by the expression

$$\widetilde{I}_{j_{(i)}} = \widetilde{d}_i \otimes \widetilde{v}_{j_{(i)}},$$

where $\widetilde{I}_{j_{(i)}}$ is the *impact* on the ith component of the attacked asset (A_j).

We use (3) below to compute the risk to the asset

$$\widetilde{R}_{j_{(i)}} = \widetilde{I}_{j_{(i)}} \otimes \widetilde{f}. \quad (3)$$

After computing the impact caused by a materialized threat on an asset, we can compute the impact transmitted from the attacked asset to its dependent assets. If A_j is the asset on which the threat has materialized and the degree of dependency of A_j with respect to A_k is $\widetilde{DD}(A_k,A_j)$, then the attack on asset A_j has an impact on A_k of $\widetilde{I}_{k_{(i)}} = \widetilde{DD}(A_k,A_j) \otimes \widetilde{d}_i \otimes \widetilde{v}_{j_{(i)}}$. Thus, the risk to asset A_k is

$$\widetilde{R}_{k_{(i)}} = \widetilde{I}_{k_{(i)}} \otimes \widetilde{f} = \widetilde{DD}(A_k,A_j) \otimes \widetilde{d}_i \otimes \widetilde{v}_{j_{(i)}} \otimes \widetilde{f}.$$

3.4. Similarity function

A *similarity function* is required to associate the resulting trapezoidal fuzzy number with an element in the linguistic term set. This function can also be used at any step of the methodology to derive the linguistic terms associated with the respective trapezoidal fuzzy numbers output to represent dependencies, accumulated values, etc.

Several authors have proposed different similarity functions, which are based on the centroid of a fuzzy number and the distance between the components of the fuzzy numbers in $TF[0,1]$, [4,15,11,5,6,28,9]. A similarity function was proposed and 30 sets of linguistic value trapezoidal fuzzy numbers were used to compare the calculation results with other previously proposed functions in [7]. Finally, a more recent similarity function was proposed in [32] and compared with the proposal reported in [7].

However, the above similarity functions are unsuitable for use in $TF[0,1]$. We use the function proposed in [22,23], which considers another parameter consisting of the ratio between the common area and the joint area under the membership functions of trapezoidal fuzzy numbers [22,23].

Given $\widetilde{A} = (a_1, a_2, a_3, a_4)$ and $\widetilde{B} = (b_1, b_2, b_3, b_4) \in TF[0,1]$, the similarity function can be defined as

- if $\max\{(a_4 - a_1), (b_4 - b_1)\} \neq 0$, then

$$S(\widetilde{A}, \widetilde{B}) = 1 - (1 - \alpha - \beta) \times \left(1 - \frac{\int_0^1 \mu_{\widetilde{A} \cap \widetilde{B}}(x)dx}{\int_0^1 \mu_{\widetilde{A} \cup \widetilde{B}}(x)dx}\right) - \alpha \frac{\sum |a_i - b_i|}{4} - \beta \frac{d\left[\left(X_{\widetilde{A}}, Y_{\widetilde{A}}\right), \left(X_{\widetilde{B}}, Y_{\widetilde{B}}\right)\right]}{M},$$

- otherwise,

$$S(\widetilde{A}, \widetilde{B}) = 1 - \left(\frac{1 - \alpha - \beta}{2} + \alpha\right) \times \frac{\sum |a_i - b_i|}{4} - \left(\frac{1 - \alpha - \beta}{2} + \beta\right) \times \frac{d\left[\left(X_{\widetilde{A}}, Y_{\widetilde{A}}\right), \left(X_{\widetilde{B}}, Y_{\widetilde{B}}\right)\right]}{M},$$

where $\alpha + \beta < 1$, $\mu_{\widetilde{\chi}}$ is the membership function of $\widetilde{\chi}$,

$$M = \max_{[0,1] \times [0,\frac{1}{2}]} \{d((x,y),(x',y'))\},$$

$$\mu_{\widetilde{A} \cap \widetilde{B}}(x) = \min_{0 \leqslant x \leqslant 1} \{\mu_{\widetilde{A}}(x), \mu_{\widetilde{B}}(x)\}, \quad \mu_{\widetilde{A} \cup \widetilde{B}}(x) = \max_{0 \leqslant x \leqslant 1} \{\mu_{\widetilde{A}}(x), \mu_{\widetilde{B}}(x)\},$$

$(X_{\widetilde{A}}, Y_{\widetilde{A}}), (X_{\widetilde{B}}, Y_{\widetilde{B}})$ are the centroids of $\widetilde{A}$ and $\widetilde{B}$, respectively, and d is a distance in $\Re^2$.

The use of this similarity measure is justified in [22,23]. Suffice is to say that $S(\widetilde{A}, \widetilde{B}) \in [0,1]$, $S(\widetilde{A}, \widetilde{B}) = S(\widetilde{B}, \widetilde{A})$, $S(\widetilde{A}, \widetilde{B}) = 1$ if and only if $\widetilde{A} = \widetilde{B}$, and $S(\widetilde{A}, \widetilde{B}) = 0$ if and only if $\widetilde{A} = (0,0,0,0)$ and $\widetilde{B} = (1,1,1,1)$.

Looking at the first example in Fig. 3, the degree of dependency of A_4 with respect to A_1 was computed in Section 2, leading to the trapezoidal fuzzy number $(0.404, 0.563, 0.719, 0.843)$, see Fig. 5. Applying the similarity function with equal weights for all three components the degree of dependency of A_4 with respect to A_1 is *Medium-High* (similarity 0.8081).

3.5. Preventive safeguards

Safeguards are measures for addressing threats. They can be procedures, such as incident management and documentation, personnel policies, technical solutions, or physical security measures at the facilities.

These safeguards can be *preventive*, if they reduce the frequency of threats; or *palliative*, if they reduce the degradation of assets caused by threats [16]. As the degree of dependency between two assets is the failure transmission probability, a special type of preventive safeguard is one that reduces dependencies between support and terminal assets.

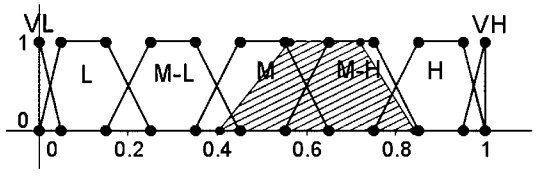

Fig. 5. Fuzzy number $(0.404, 0.563, 0.719, 0.843)$.

The effect induced by a safeguard on the failure transmission probability between two assets A_u and A_v can also be defined as a linguistic term, which is represented by a fuzzy number $\widetilde{e} \in TF[0,1]$. So if the degree of direct dependency between the assets A_u and A_v is $\widetilde{dd}(A_u, A_v)$, then, when we implement a safeguard with effect $\widetilde{e}$, the degree of direct dependency is reduced to

$$\widetilde{dd}(A_u, A_v) \otimes (\widetilde{1} \ominus \widetilde{e}),$$

where $\ominus$ denotes the usual subtraction operation between trapezoidal fuzzy numbers, i.e., $(a_1, a_2, a_3, a_4) \ominus (b_1, b_2, b_3, b_4) = (a_1 - b_4, a_2 - b_3, a_3 - b_2, a_4 - b_1)$.

We consider the set of safeguards that block direct failure transmission between A_u and A_v, $S^{u,v}$. Each safeguard $S_p^{u,v} \in S^{u,v}$ has a monetary cost $c_p^{u,v}$ and an effect $\widetilde{e}_p^{u,v}$ on $\widetilde{dd}(A_u, A_v)$.

The problem of keeping the failure transmission probabilities among support and terminal assets at an acceptable level with minimal costs can be represented as:

$$\begin{aligned} &\min \sum_{u,v} \sum_{p} c_p^{u,v} x_p^{u,v} \\ &s.t. \\ &\widetilde{DD}(A_i, A_k) \leqslant \widetilde{U}_{ik} \ \forall i,k \\ &x_p^{u,v} \in \{0,1\} \forall u,v,p, \end{aligned} \tag{4}$$

where i and k in the first set of constraints refer to non-terminal and terminal assets, respectively, $\widetilde{U}_{ik}$ is a residual value accepted by the experts, $x_p^{u,v}$ are the decision variables ($x_p^{u,v} = 1$ means that safeguard $S_p^{u,v}$ is selected), and $\widetilde{DD}(A_i, A_k)$ is reassessed replacing values $\widetilde{dd}(A_u, A_v)$ by the affected values regarding the selected safeguards:

$$\widetilde{dd}(A_u, A_v) \otimes \left[\bigotimes_p (\widetilde{1} - \widetilde{e}_p^{u,v})\right],$$

where A_u and A_v are two consecutive assets connected by an arc in some path between A_i and A_k.

Note that the fact that the usual order in $TF[0,1]$ is a partial order constitutes a very restrictive constraint in our optimization problem, so we will use the similarity function, S, introduced in the previous section, to relax this constraint.

If we define a threshold $\alpha \in [0,1]$, the constraint $\widetilde{DD}(A_i, A_k) \leqslant \widetilde{U}_{ik}$ $\forall i,k$ can be replaced by $S(\widetilde{DD}(A_i, A_k), \widetilde{U}_{ik}) \geqslant \alpha$ in (4). Thus, the restrictiveness of the constraint increases proportionally to the threshold value and the feasible solution set will be composed of solutions that verify these softened/relaxed constraints.

Remember that indirect dependencies are recursively computed following the algorithm described in Section 3.1. Thus, the degree of dependency of the support assets further away from the terminals can be computed from the degree of dependency of the closest assets. Therefore, the problem can be solved in a stage-wise manner, and observes the *principle of optimality* as required in dynamic programming: given an optimal sequence of decisions, every subsequence is, in turn, optimal. Then, we proceed as follows:

- Let L_0 be the set of terminal assets. Identify safeguards that minimize costs keeping the degrees of dependency between assets in L_0 at an acceptable level.
- Consider L_1 including support assets whose children belong to L_0 only. Identify safeguards that minimize costs keeping the degrees of dependency on their children at an acceptable level.
- Consider L_2 including support assets whose children belong to $L_0 \cup L_1$ only. Identify safeguards that minimize costs keeping the degrees of dependency over L_0 under an

acceptable level. Note that the degrees of indirect dependency from the children of L_2 to terminal assets have already been computed in the previous stage, so we just need to identify the direct degree of dependency on assets in $L_0 \cup L_1$.

- ...
- Consider L_i including support assets whose children belong to $L_0 \cup L_1 \cup \ldots \cup L_{i-1}$ only. Identify safeguards that minimize costs keeping the degrees of dependency on L_0 under an acceptable level. Note that again we just need to identify the direct degree of dependency on assets of $L_0 \cup \ldots \cup L_{i-1}$.

Simulated annealing (SA) [14,3] is applied in each step of the algorithm to derive the optimal selection of safeguards from optimization problems in (4).

The basic idea of SA is as follows. An initial feasible solution is randomly generated. In each iteration a new solution is randomly generated from the neighborhood of the current solution. If the new solution is better than the current one, then the algorithm moves to that solution, otherwise there is some probability of a movement to the new solution. Accepting worse solutions allows for a more extensive search for the optimal solution and avoids trapping in local optima in early iterations.

The probability of accepting a worse movement is a function of both a temperature factor (t) and the change in the cost function. The initial value of t is high, which leads to a diversified search, since practically all movements are allowed. As t decreases, the probability of accepting a worse movement falls. If t is zero, then only better movements will be accepted, which makes SA work like hill climbing.

4. An illustrative example

We consider an administrative unit that uses in-house and third-party information systems internally to provide public information services (electronic government) [16]. Alarmed by potential security threats existing in the internet and taking into account that a service failure would cause serious damage to the unit's operation and prestige, a risk analysis and management project was launched.

The project scope was confined to the personal and remote electronic processing service, as well as the security of the information handled. With regard to the equipment, both machine and communications networks were analysed.

The service was provided by a computer database application accessed via a local user identification that controls access privileges. The processing includes a request (and data entry) phase and a response (and data delivery) phase. Users make their request and await a notification to collect the reply. The notification was sent by registered mail in the case of personal processing, and by email in the case of remote processing.

A centralised archive and document recovery service was provided by an intranet. Users accessed it through a local Web interface that connects via a private virtual network with a remote server, with users identified by their identity card number. This service was only available to the unit personnel and to the virtual employee who provides the remote formality service.

The unit had various PCs on its premises. The equipment had no removable media of any type: diskette, CD, DVD, USB, etc., and a medium-sized, general-purpose server was available as file, electronic mail, database and web server.

A local area network was available with an ADSL internet connection via a firewall that limited the communication. Remote processing, e-mail, information access and a private virtual network with the central archive services were provided via the internet connection.

A *risk analysis stage* revealed the assets and the asset dependencies shown in Fig. 6. A more detailed description of this stage is provided in [16], where the MAGERIT methodology is used to analyse the problem. Therefore, Boolean values were originally used to indicate whether or not any dependencies existed regardless of the degree of dependency. The computations were made using PILAR [18] software that implements the MAGERIT methodology.

The following 11 assets were considered: *processing in person* (presential-proc), *remote processing* (remote-proc), *current files* (current-f), *e-mail* (mail), *central historical archive* (archive), *processing of files* (files-proc), *work stations* (wrk-stat), *server* (server), *firewall* (firewall), *local network* (LAN), and *internet connection* (internet). Note that three out of the eight assets were terminal: *current files*, *processing in person* and *remote processing*.

Following the methodology proposed in this paper, we first consider the set of linguistic terms with their respective trapezoidal fuzzy numbers shown in Table 1 and Fig. 4. Next, experts give linguistic terms to express the influences between IS assets, see Fig. 6. Note that only two dependencies are high, (*server*, *archive*) and (*server*, *current-f*), while two are medium-high (*internet*, *archive*) and (*archive*, *current-f*).

Then, we compute the degree of asset dependency on terminal assets. First, the degree of dependency for assets that directly influence terminal assets is immediate, see Table 3. Table 4 shows computations to derive the *firewall*, *internet* and *server* dependencies with respect to the three terminal assets, whereas Table 5 shows the resulting dependencies of non-terminal with respect to the three terminal assets.

Next, experts assign linguistic terms for each terminal asset component, see Table 6. Note that *authenticity* and *traceability* have been split into two new components in this example each, corresponding to data and services, respectively. Consequently, seven components will be considered for each asset, that is, *confidentiality* (Confid.), *integrity* (Integr.), *data authenticity* (D. Aut.), *service*

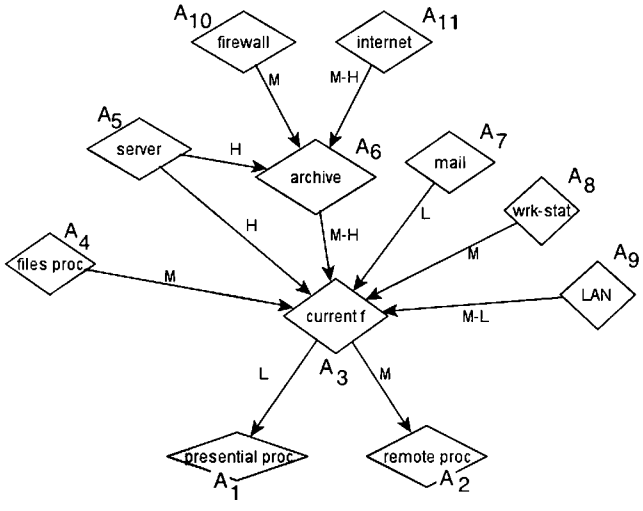

Fig. 6. Asset dependencies in an IS.

Table 3
Immediate dependency degree computation.

	presential-proc	*current-f*	*remote-proc*
files-proc	M⊗L	M	M⊗M
archive	M–H⊗L	M–H	M–H⊗M
email	L⊗L	L	L⊗M
wrk-stat	M⊗L	M	M⊗M
LAN	M–L⊗L	M–L	M–L⊗M

Table 4
Accumulated dependencies for *firewall*, *internet* and *server*.

	presential-pro	*current-f*	*remote-proc*
firewall	M⊗M–H⊗L	M⊗M–H	M⊗M–H⊗M
internet	M–H⊗M–H⊗L	M–H⊗M–H	M–H ⊗M–H⊗M
server	[H⊕(H⊗M–H)]⊗L	H⊕(H⊗M–H)	[H⊕(H⊗M–H)]⊗M

authenticity (S. Aut.), *data traceability* (D. Tra.), *service traceability* (S. Tra.) and *availability* (Avail.).

Accumulated values are computed for non-terminal assets by means of (2), see Table 7. For example, the accumulated value for the *archive* asset in each component is computed as follows:

$$\begin{aligned}\widetilde{v}_{archive_{(1)}} &= [(\mathrm{M}-\mathrm{H}\otimes \mathrm{L})\otimes v_{presential-proc_{(1)}}]+[\mathrm{M}-\mathrm{H}\otimes v_{current-f_{(1)}}]\\ &\quad +[(\mathrm{M}-\mathrm{H}\otimes \mathrm{M})\otimes v_{remote-proc_{(1)}}]\\ &= (0.302,0.422,0.562,0.722)\end{aligned}$$

$$\begin{aligned}\widetilde{v}_{archive_{(2)}} &= [(\mathrm{M}-\mathrm{H}\otimes \mathrm{L})\otimes v_{presential-proc_{(2)}}]+[\mathrm{M}-\mathrm{H}\otimes v_{current-f_{(2)}}]\\ &\quad +[(\mathrm{M}-\mathrm{H}\otimes \mathrm{M})\otimes v_{remote-proc_{(2)}}]\\ &= (0.192,0.292,0.412,0.552)\end{aligned}$$

...

$$\begin{aligned}\widetilde{v}_{archive_{(7)}} &= [(\mathrm{M}-\mathrm{H}\otimes \mathrm{L})\otimes v_{presential-proc_{(7)}}]+[\mathrm{M}-\mathrm{H}\otimes v_{current-f_{(7)}}]\\ &\quad +[(\mathrm{M}-\mathrm{H}\otimes \mathrm{M})\otimes v_{remote-proc_{(7)}}]\\ &= (0.28,0.086,0.197,0.352)\end{aligned}$$

The MAGERIT methodology originally used a 1–10 integer scale to valuate asset components, where 1 and 10 were the least and most important values, respectively. Assignment criteria are officially described in the methodology [16]. We have translated the above values into the fuzzy linguistic scale, yielding the values for the three terminal assets shown in Table 6.

Now let us consider a threat to the *archive* asset with a degradation (provided by experts) $\widetilde{D}$ = (H, L, VL, M, M–H, VH, H). Table 7, shows the seven-component valuation of this asset, and the impact on the asset is computed by multiplying each component of the above vectors, see Table 8.

Note that the similarity function can be used at any step of the methodology to derive the linguistic term associated with the trapezoidal fuzzy number output respectively representing accumulated dependency, values, etc. However, trapezoidal fuzzy numbers will be used throughout the steps of the methodology since the use of linguistic terms would mean a loss of information.

Using equal weights and the infinity distance measure in the similarity function, see Section 3.4, then the impact on the components the *archive* asset is (M, M–L, VL, L, M–L, M–L, L).

Next, experts assigned a high frequency (H) to the threat. Risks were then computed using (3), which yielded the values listed in Table 8. Impacts and risk can then be computed for assets that influence the attacked asset (*archive*), that is, *server*, *firewall* and *internet*, see Table 8.

Using the similarity function the *risk* to *archive* asset in each component is (M, L, VL, L, M–L, M–L, L). Finally, Table 9 shows the linguistic terms associated with the risk to the attacked asset and to assets that influence the attacked asset.

Now, we consider the set of available safeguards of failure transmission between support assets shown in Table 10, and the fuzzy threshold $\widetilde{U} = (0, 0, 0.05, 0.1)$ below which the degree of

Table 6
Linguistic terms for components in terminal assets.

	presential-proc	*current-f*	*remote-proc*
Confidentiality		M–H	
Integrity		M	
Data authenticity		M	
Service authenticity	M–H		M–H
Data traceability		M	
Service traceability	M		M
Availability	M		M–L

Table 7
Accumulated values for non-terminal assets.

Comp.	*files-proc*	*archive*
Confid.	(0.192, 0.292, 0.412, 0.552)	(0.302, 0.422, 0.562, 0.722)
Integr.	(0.122, 0.202, 0.302, 0.422)	(0.192, 0.292, 0.412, 0.552)
D. Aut.	(0.122, 0.202, 0.302, 0.422)	(0.192, 0.292, 0.412, 0.552)
S. Aut.	(0.067, 0.144, 0.274, 0.447)	(0.105, 0.207, 0.367, 0.565)
D. Tra.	(0.122, 0.202, 0.302, 0.422)	(0.192, 0.292, 0.412, 0.552)
S. Tra.	(0.042, 0.100, 0.204, 0.351)	(0.067, 0.144, 0.274, 0.447)
Avail.	(0.018, 0.060, 0.146, 0.275)	(0.028, 0.086, 0.197, 0.352)
	email	*wrk-stat*
Confid.	(0.0, 0.032, 0.112, 0.212)	(0.192, 0.292, 0.412, 0.552)
Integr.	(0.0, 0.022, 0.082, 0.162)	(0.122, 0.202, 0.302, 0.422)
D. Aut.	(0.0, 0.022, 0.082, 0.162)	(0.122, 0.202, 0.302, 0.422)
S. Aut.	(0.0, 0.016, 0.077, 0.183)	(0.067, 0.144, 0.2740.447)
D. Tra.	(0.0, 0.022, 0.082, 0.162)	(0.122, 0.202, 0.302, 0.422)
S. Tra.	(0.0, 0.011, 0.057, 0.141	(0.042, 0.100, 0.204, 0.351)
Avail.	(0.0, 0.006, 0.040, 0.1110	(0.018, 0.060, 0.146, 0.275)
	LAN	*firewall*
Confid.	(0.082, 0.162, 0.262, 0.382)	(0.105, 0.190, 0.309, 0.469)
Integr.	(0.052, 0.112, 0.192, 0.292)	(0.067, 0.131, 0.226, 0.359)
D. Aut.	(0.052, 0.112, 0.192, 0.292)	(0.067, 0.131, 0.226, 0.359)
S. Aut.	(0.028, 0.080, 0.178, 0.320)	(0.037, 0.094, 0.208, 0.386)
D. Tra.	(0.052, 0.112, 0.192, 0.292)	(0.067, 0.131, 0.226, 0.359)
S. Tra.	(0.018, 0.055, 0.131, 0.249)	(0.023, 0.065, 0.154, 0.302)
Avail.	(0.007, 0.033, 0.094, 0.195)	(0.010, 0.039, 0.110, 0.236)
	internet	*server*
Confid.	(0.166, 0.274, 0.625, 0.614)	(0.442, 0.587, 0.75, 0.85)
Integr.	(0.105, 0.190, 0.309, 0.469)	(0.281, 0.406, 0.55, 0.65)
D. Aut.	(0.105, 0.190, 0.309, 0.469)	(0.281, 0.406, 0.55, 0.65)
S. Aut.	(0.058, 0.135, 0.280, 0.491)	(0.132, 0.264, 0.478, 0.647)
D. Tra.	(0.105, 0.190, 0.309, 0.469)	(0.281, 0.406, 0.55, 0.65)
S. Tra.	(0.037, 0.094, 0.208, 0.386)	(0.084, 0.183, 0.360, 0.516)
Avail.	(0.015, 0.056, 0.149, 0.303)	(0.036, 0.101, 0.259, 0.407)

Table 5
Trapezoidal fuzzy numbers representing degree of dependency.

	presential-proc	*current-f*	*remote-proc*
files-proc	(0, 0.022, 0.082, 0.162)	(0.35, 0.45, 0.55, 0.65)	(0.122, 0.202, 0.302, 0.422)
archive	(0, 0.032, 0.112, 0.212)	(0.55, 0.65, 0.75, 0.85)	(0.192, 0.292, 0.412, 0.552)
email	(0, 0.002, 0.022, 0.062)	(0, 0.05, 0.15, 0.25)	(0, 0.022, 0.082, 0.162)
wrk-stat	(0, 0.022, 0.082, 0.162)	(0.35, 0.45, 0.55, 0.65)	(0.122, 0.202, 0.302, 0.422)
LAN	(0, 0.012, 0.052, 0.112)	(0.15, 0.25, 0.35, 0.45)	(0.052, 0.112, 0.192, 0.292)
firewall	(0 0.014, 0.061, 0.138)	(0.192, 0.292, 0.412, 0.552)	(0.067, 0.131, 0.226, 0.359)
internet	(0, 0.021, 0.084, 0.18)	(0.302, 0.422, 0.562, 0.722)	(0.105, 0.190, 0.309, 0.469)
server	(0, 0.046, 0.147, 0.25)	(0.853, 0.932, 0.985, 1)	(0.298, 0.419, 0.542, 0.65)

Table 8
Impacts on and risks to *archive*, *server*, *firewall* and *internet* assets.

Comp.	Impact (*archive*)	Risk (*archive*)
Confid.	(0.227,0.359,0.534,0.722)	(0.170,0.305,0.508,0.722)
Integr.	(0,0.015,0.062,0.138)	(0,0.012,0.059,0.138)
D. Aut.	(0,0,0,0.028)	(0,0,0,0.028)
S. Aut.	(0.037,0.093,0.202,0.367)	(0.028,0.079,0.192,0.367)
D. Tra.	(0.106,0.190,0.309,0.469)	(0.079,0.162,0.294,0.470)
S. Tra.	(0.064,0.144,0.275,0.448)	(0.048,0.123,0.261,0.448)
Avail.	(0.022,0.074,0.187,0.352)	(0.016,0.063,0.178,0.352)
	Impact (*server*)	Risk (*server*)
Confid.	(0.283,0.465,0.702,0.85)	(0.212,0.396,0.667,0.85)
Integr.	(0,0.019,0.081,0.162)	(0,0.016,0.077,0.162)
D. Aut.	(0,0,0,0.0325)	(0,0,0,0.032)
S. Aut.	(0.040,0.111,0.259,0.421)	(0.030,0.094,0.246,0.421)
D. Tra.	(0.132,0.247,0.407,0.552)	(0.099,0.201,0.386,0.552)
S. Tra.	(0.068,0.171,0.355,0.516)	(0.051,0.145,0.337,0.516)
Avail.	(0.023,0.081,0.243,0.407)	(0.017,0.069,0.230,0.407)
	Impact (*firewall*)	Risk (*firewall*)
Confid.	(0.028,0.073,0.1612,0.305)	(0.021,0.062,0.154,0.305)
Integr.	(0,0.002,0.019,0.058)	(0,0.002,0.018,0.058)
D. Aut.	(0,0,0,0.012)	(0,0,0,0.012)
S. Aut.	(0.005,0.019,0.063,0.163)	(0.003,0.016,0.06,0.163)
D. Tra.	(0.013,0.038,0.094,0.198)	(0.010,0.033,0.089,0.198)
S. Tra.	(0.008,0.029,0.085,0.196)	(0.006,0.025,0.081,0.196)
Avail.	(0.003,0.015,0.058,0.154)	(0.002,0.013,0.055,0.154)
	Impact (*internet*)	Risk (*internet*)
Confid.	(0.069,0.152,0.301,0.522)	(0.051,0.129,0.286,0.522)
Integr.	(0,0.006,0.035,0.1)	(0,0.005,0.033,0.01)
D. Aut.	(0,0,0,0.02)	(0,0,0,0.02)
S. Aut.	(0.011,0.04,0.116,0.272)	(0.008,0.034,0.11,0.272)
D. Tra.	(0.032,0.080,0.174,0.339)	(0.024,0.068,0.165,0.339)
S. Tra.	(0.019,0.061,0.156,0.329)	(0.015,0.052,0.149,0.329)
Avail.	(0.007,0.031,0.107,0.258)	(0.005,0.027,0.101,0.258)

Table 9
Linguistic terms for risks to assets.

Component	*archive*	*firewall*	*internet*	*server*
Confidentiality	M	L	M–L	M
Integrity	L	VL	VL	L
Data authenticity	VL	VL	VL	VL
Service authenticity	L	L	L	L
Data traceability	M–L	L	L	M–L
Service traceability	M–L	L	L	M–L
Availability	L	L	L	L

dependency between all assets and terminal assets will be acceptable, and let $\alpha = 0.95$.

Dynamic programming is then executed as follows.

Stage 0: L_0 = {*presential-proc* (A_1), *remote-proc* (A_2), *current-f* (A_3)}, since there are three terminal assets in the IS. We identify safeguards for (A_3) that minimize costs keeping the degrees of dependency on (A_1) and (A_2) at acceptable levels, $S(\widetilde{DD}(A_3,A_1), \widetilde{U}) \geqslant 0.95$ and $S(\widetilde{DD}(A_3,A_2), \widetilde{U}) \geqslant 0.95$, respectively.

Regarding asset A_3, solutions are represented by the vector $x^{3,1} = (x_1^{3,1}, \ldots, x_8^{3,1})$, see Table 10, where $x_p^{3,1} = 1$ if the safeguard $S_p^{3,1}$ is selected. $x^{3,2} = (x_1^{3,2}, \ldots, x_{10}^{3,2})$ is considered for asset A_2. Both safeguards sets are independently selected by solving the following optimization problems:

$$\begin{array}{ll} \min & c_1^{3,1}x_1^{3,1} + \ldots + c_8^{3,1}x_8^{3,1} \\ s.t. & \\ S(\widetilde{DD}(A_3,A_1), \widetilde{U}) \geqslant 0.95 & \\ x_p^{3,1} \in \{0,1\}, p = 1,\ldots,8 & \end{array} \qquad \begin{array}{ll} \min & c_1^{3,2}x_1^{3,2} + \ldots + c_{10}^{3,2}x_{10}^{3,2} \\ s.t. & \\ S(\widetilde{DD}(A_3,A_2), \widetilde{U}) \geqslant 0.95 & \\ x_q^{3,2} \in \{0,1\}, q = 1,\ldots,10 & \end{array}$$

The optimal solution output by using simulated annealing and the associated costs are $x^{3,1^*} = (0,0,1,0,0,0,0,1)$ and $x^{3,2^*} = (0,0,1,0,0,0,1,1,0,0)$, with costs 220 and 646, respectively, see Table 11.

Table 10
Available safeguards.

Asset	Safeguards (Tag ($S_p^{u,v}$), effect ($e_p^{u,v}$), cost ($c_p^{u,v}$))
current-f	$S^{3,1}$: {($S_1^{3,1}$,M,250),($S_2^{3,1}$,L,120),($S_3^{3,1}$,L,100), ($S_4^{3,1}$,M–L,179), ($S_5^{3,1}$,M,225),($S_6^{3,1}$,M–L,160),($S_7^{3,1}$,L,100), ($S_8^{3,1}$,M–L,120)}
	$S^{3,2}$: {($S_1^{3,2}$,L,100),($S_2^{3,2}$,M–L,127),($S_3^{3,2}$,M,234), ($S_4^{3,2}$,L,180),($S_5^{3,2}$,L,147), ($S_6^{3,2}$,L,127),($S_7^{3,2}$,M,234),($S_8^{3,2}$,M,178), ($S_9^{3,2}$,L,220), ($S_{10}^{3,2}$,M–L,170)}
files-proc	$S^{4,3}$: {($S_1^{4,3}$,M–L,196),($S_2^{4,3}$,L,108),($S_3^{4,3}$,M,205), ($S_4^{4,3}$,M–H,310), ($S_5^{4,3}$,M,245),($S_6^{4,3}$,L,169),($S_7^{4,3}$,M–L,208), ($S_8^{4,3}$,M,254)}
firewall	$S^{10,6}$: {($S_1^{10,6}$,M,234),($S_2^{10,6}$,M,267),($S_3^{10,6}$,M,215), ($S_4^{10,6}$,M–H,280), ($S_5^{10,6}$,M–L,200),($S_6^{10,6}$,M–H,295),($S_7^{10,6}$,L, 167),($S_8^{10,6}$,M,203)}
internet	$S^{11,6}$: {($S_1^{11,6}$,M–H,302),($S_2^{11,6}$,M–L,129),($S_3^{11,6}$,M, 235), ($S_4^{11,6}$,M,256),($S_5^{11,6}$,M,231),($S_6^{11,6}$,L,178), ($S_7^{11,6}$,M–H,289)}
server	$S^{5,3}$: {($S_1^{5,3}$,M,207),($S_2^{5,3}$,L,109),($S_3^{5,3}$,M–H,245), ($S_4^{5,3}$,M,267), ($S_5^{5,3}$,M–L,102)}
	$S^{5,6}$: {($S_1^{5,6}$,M,238),($S_2^{5,6}$,L,134),($S_3^{5,6}$,M–L,256), ($S_4^{5,6}$,L,111),($S_5^{5,6}$,M,208)}
archive	$S^{6,3}$: {($S_1^{6,3}$,M,248),($S_2^{6,3}$,M,224),($S_3^{6,3}$,M,200), ($S_4^{6,3}$,M–L,167), ($S_5^{6,3}$,L,110),($S_6^{6,3}$,M–H,256)}
wrk-stat	$S^{8,3}$: {($S_1^{8,3}$,M,257),($S_2^{8,3}$,M,234),($S_3^{8,3}$,L,189), ($S_4^{8,3}$,M,236), ($S_5^{8,3}$,M,204),($S_6^{8,3}$,L,104)}
mail	$S^{9,3}$: {($S_1^{9,3}$,L,110),($S_2^{9,3}$,L,124),($S_3^{9,3}$,M–L,143), ($S_4^{9,3}$,M,206), ($S_5^{9,3}$,M,237),($S_6^{9,3}$,L,170)}
LAN	$S^{7,3}$: {($S_1^{7,3}$,M,234),($S_2^{7,3}$,L,201),($S_3^{7,3}$,M,245), ($S_4^{7,3}$,L,178), ($S_5^{7,3}$,M,205),($S_6^{7,3}$,M,200)}

Stage 1: L_1 ={*files-proc* (A_4), *archive* (A_6), *mail* (A_7), *wrk-stat* (A_8), *LAN* (A_9)}. We identify safeguards that minimize costs keeping the degrees of direct dependencies between assets in L_1 and terminal assets at, $S(\widetilde{DD}(A_i,A_1), \widetilde{U}) \geqslant 0.95, S(\widetilde{DD}(A_i,A_2), \widetilde{U}) \geqslant 0.95$ and $S(\widetilde{DD}(A_i,A_3), \widetilde{U}) \geqslant 0.95$, with $A_i \in L_1$.

Note that $\widetilde{DD}(A_4,A_1) = \widetilde{dd}(A_4,A_3) \otimes \widetilde{DD}(A_3,A_1)$ and the value of $\widetilde{DD}(A_3,A_1)$ was computed in the previous stage. Analogously, $\widetilde{DD}(A_4,A_2) = \widetilde{dd}(A_4,A_3) \otimes \widetilde{DD}(A_3,A_2)$, and the value of $\widetilde{DD}(A_3,A_2)$ was also computed in the previous stage.

Five optimization problems have to be solved to select safeguards for each asset in L_1. For instance, the optimization problem for *files_proc* (A_4) is

Table 11
Optimal selection of safeguards and costs.

Asset	Optimal solution	Cost	Stage
current-f	$x^{3,2^*} = (0,0,1,0,0,0,1,1,0,0)$	646	0
	$x^{3,1^*} = (0,0,1,0,0,0,0,1)$	220	0
files-proc	$x^{4,3^*} = (0,1,1,1,0,0,0,0)$	623	1
archive	$x^{6,3^*} = (0,1,1,0,0,1)$	680	1
mail	$x^{7,3^*} = (0,0,0,1,0,0)$	206	1
wrk-stat	$x^{8,3^*} = (0,1,0,1,1,0)$	674	1
LAN	$x^{9,3^*} = (0,0,0,1,1,1)$	583	1
server	$x^{5,3^*} = (1,0,1,1,1)$	1267	2
	$x^{5,6^*} = (1,0,0,0,1)$		2
firewall	$x^{10,6^*} = (0,0,0,0,0,0,0,0,0,0)$	0	2
internet	$x^{11,6^*} = (0,0,0,0,0,0,0,0)$	0	2
		4899	

$$\begin{aligned}
&\min \quad c_1^{4,3}x_1^{4,3} + \cdots + c_8^{4,3}x_8^{4,3}\\
&s.t.\\
&S(\widetilde{DD}(A_4,A_1),\widetilde{U}) \geqslant 0.95\\
&S(\widetilde{DD}(A_4,A_2),\widetilde{U}) \geqslant 0.95\\
&S(\widetilde{DD}(A_4,A_3),\widetilde{U}) \geqslant 0.95\\
&x_p^{4,3} \in \{0,1\}, p = 1,\ldots,8
\end{aligned}$$

The optimal solution output by using simulated annealing and the associated costs are $x^{4,3^*} = (0,1,1,1,0,0,0,0)$ and 623, respectively, see Table 11.

Stage 2: L_2 ={*server* (A_5), *firewall* (A_{10}), *internet* (A_{11})}. Now, we identify safeguards that minimize costs keeping the degrees of direct dependencies between assets in L_2 and terminal assets at levels obtained in Stage 1.

The degree of dependency of the *server* asset (A_5) on terminal assets can be computed by

$$\begin{aligned}
\widetilde{DD}(A_5,A_1) &= \left[\left(\widetilde{dd}(A_5,A_6)\otimes\widetilde{DD}(A_6,A_3)\right)\oplus\widetilde{dd}(A_5,A_3)\right]\otimes\widetilde{DD}(A_3,A_1),\\
\widetilde{DD}(A_5,A_2) &= \left[\left(\widetilde{dd}(A_5,A_6)\otimes\widetilde{DD}(A_6,A_3)\right)\oplus\widetilde{dd}(A_5,A_3)\right]\otimes\widetilde{DD}(A_3,A_2),\\
\widetilde{DD}(A_5,A_3) &= \left(\widetilde{dd}(A_5,A_6)\otimes\widetilde{DD}(A_6,A_3)\right)\oplus\widetilde{dd}(A_5,A_3),
\end{aligned}$$

respectively, and $\widetilde{DD}(A_3,A_1)$ and $\widetilde{DD}(A_3,A_2)$ were computed in Stage 0, whereas $\widetilde{DD}(A_6,A_3)$ was computed in Stage 1.

The corresponding optimization problem for *server* (A_5) is

$$\begin{aligned}
&\min \quad c_1^{5,3}x_1^{5,3} + \ldots + c_5^{5,3}x_5^{5,3} + c_1^{5,6}x_1^{5,6} + \ldots + c_5^{5,6}x_5^{5,6}\\
&s.t.\\
&S(\widetilde{DD}(A_5,A_1),\widetilde{U}) \geqslant 0.95\\
&S(\widetilde{DD}(A_5,A_2),\widetilde{U}) \geqslant 0.95\\
&S(\widetilde{DD}(A_5,A_3),\widetilde{U}) \geqslant 0.95\\
&x_p^{5,3}, x_p^{5,6} \in \{0,1\}, p = 1,\ldots,5,
\end{aligned}$$

and the optimal solutions output using simulated annealing are $x^{5,3^*} = (1,0,1,1,1)$ and $x^{5,6^*} = (1,0,0,0,1)$ with a cost of 1267, see Table 11.

Table 11 shows the optimal solutions representing the selection of safeguards for assets throughout the application of dynamic programming and simulated annealing and the respective costs, whereas Table 12 shows the degree of dependency of assets on terminal assets after the implementation of the selected safeguards.

Note that no safeguards are selected for the *firewall* (A_{10}) and *internet* (A_{11}) assets, see Table 12. The reason is that the implementation of optimal safeguards for the *archive* asset (A_6) in *Stage 1* reduce the degree of dependency of that asset on terminal assets, see Table 12, row 3. Consequently, the degree of dependency of the *firewall* (A_{10}) and *internet* (A_{11}) assets, which are connected only to the *archive* asset (see Fig. 6), on terminal assets is so low at that point that it is unnecessary to implement any safeguards for those assets, and no money has to be spent.

Table 12
Degree of dependencies after the implementation of safeguards.

Asset	*Presential proc*	*current f*	*remote proc*
current f	(0,0.002,0.08,0.16)	1	(0,0.04,0.09,0.17)
files proc	(0,0.01,0.05,0.13)	(0.01,0.04,0.10,0.19)	(0,0.01,0.05,0.11)
archive	(0,0.01,0.05,0.13)	(0.01,0.04,0.10,0.19)	(0,0.01,0.05,0.11)
mail	(0,0,0.01,0.05)	(0,0.02,0.08,0.16)	(0,0,0.01,0.04)
wrk-stat	(0,0.01,0.05,0.13)	(0.01,0.04,0.09,0.17)	(0,0.01,0.05,0.11)
LAN	(0,0,0.03,0.09)	(0.01,0.04,0.10,0.19)	(0,0.01,0.03,0.08)
server	(0,0,0,0.03)	(0,0.03,0.10 0.22)	(0,0,0,0.03)
firewall	(0,0,0.02,0.08)	(0,0.01,0.05,0.12)	(0,0,0.02,0.07)
internet	(0,0,0.03,0.11)	(0,0.02,0.07,0.16)	(0,0,0.03,0.09)

Table 13
Safeguards and costs for the new thershold.

Asset	Optimal solution	Cost	Stage
current-f	$x^{3,2^*} = (1,1,1,0,0,0,0,1,0,0)$	639	0
	$x^{31^*} = (0,0,0,0,0,0,0,1)$	120	0
files-proc	$x^{4,3^*} = (0,0,1,1,0,0,0,0)$	515	1
archive	$x^{6,3^*} = (0,1,1,0,0,1)$	680	1
mail	$x^{7,3^*} = (0,0,1,0,0,0)$	143	1
wrk-stat	$x^{8,3^*} = (0,1,0,1,1,0)$	674	1
LAN	$x^{9,3^*} = (0,0,0,0,1,1)$	405	1
server	$x^{5,3^*} = (1,0,1,1,1)$	1267	2
	$x^{5,6^*} = (1,0,0,0,1)$		2
firewall	$x^{10,6^*} = (0,0,0,0,0,0,0,0)$	0	2
internet	$x^{11,6^*} = (0,0,0,0,0,0,0,0)$	0	2
		4443	

If we consider that the fuzzy threshold for keeping the failure transmission probabilities among support and terminal assets at an acceptable level is now $\widetilde{U} = (0,0,0.075,0.15)$, then costs associated with selected safeguards would decrease to 4443, as was expected since a weaker threshold is used.

Table 13 shows the resulting selection of preventive safeguards and the respective costs. We have marked the differences regarding the solutions in Table 11 in bold. Note that the selection of safeguards is the same for *archive*, *wrk-stat*, *server*, *firewall*, and *internet*, five safeguards are no longer necessary and three additional safeguards are now selected for *current-f* and *mail*.

5. Conclusions and future research

We have developed a fuzzy risk analysis model for information systems that conforms to international standards, particularly the MAGERIT methodology. The model improves this methodology and other existing methodologies since it includes uncertainty about the assessments by means of linguistic terms, which correspond with trapezoidal fuzzy numbers. The proposed methodology makes computations on the basis of trapezoidal fuzzy numbers to accumulate dependencies between assets and asset valuations and to determine impacts and risk from threat-related degradation and threat frequency, respectively. Moreover, similarity functions can be used at any step in the methodology to derive a linguistic term for the trapezoidal fuzzy number output.

A model for selecting preventive safeguards to reduce risks based on the reduction of the degree of dependency between support assets and terminal assets has also been proposed. The aim is to select safeguards that minimize costs while keeping the risk at acceptable levels.

Dynamic programming combined with simulated annealing was used because of the special structure of the constraint set. This leads to a more computationally efficient solution to the safeguard selection problem.

We have assumed that the threat frequencies are represented by linguistic terms (trapezoidal fuzzy numbers). However, these frequencies might change depending on a number of variables in the context of the information system. In the future, we will intend to build a fuzzy control system to establish different alarm levels according to these variable values.

In the future, we also intend to consider the problem of selecting preventive safeguards that minimize risks to information systems in the line with a budget allocation.

References

[1] C. Alberts, A. Dorofee, Managing Information Security Risks: The OCTAVE Approach, Addison-Wesley, New York, 2002.

[2] J. Alcalá-Fernández, R. Alcalá, M.J. Gacto, F. Herrera, Learning the membership function contexts for mining fuzzy association rules by using genetic algorithms, Fuzzy Sets Syst. 160 (2009) 905–921.
[3] V. Cerny, Thermodynamical approach to the traveling salesman problem: an efficient simulation algorithm, J. Optim. Theor. Appl. 45 (1985) 41–51.
[4] S.-M. Chen, New methods for subjective mental workload assessment and fuzzy risk analysis, Cybernetics Syst. 27 (1996) 449–472.
[5] S.-J. Chen, S.-M. Chen, A new method to measure the similarity between fuzzy numbers, in: Proc. 10th IEEE Int. Conf. Fuzzy Syst., 2001, pp. 208–214.
[6] S.-J. Chen, S.-M. Chen, Fuzzy risk analysis based on similarity measures of generalized fuzzy numbers, IEEE Trans. Fuzzy Syst. 11 (2003) 45–56.
[7] S.-J. Chen, S.-M. Chen, Fuzzy risk analysis based on the ranking of generalized trapezoidal fuzzy numbers, Appl. Intell. 26 (2007) 1–11.
[8] CCTA Risk Analysis and Management Method (CRAMM), Version 5.0, Central Computing and Telecommunications Agency (CCTA), London.
[9] S.R. Hejazi, A. Doostparast, S.M. Hosseini, An improved fuzzy risk analysis based on a new similarity measures of generalized fuzzy numbers, Expert Syst. Appl. 38 (2011) 9179–9185.
[10] F. Herrera, L. Martínez, A 2-tuple fuzzy linguistic representation model for computing with words, IEEE Trans. Fuzzy Syst. 8 (2000) 746–752.
[11] C.H. Hsieh, S.H. Chen, Similarity of generalized fuzzy numbers with graded mean integration representation, in: Proc. 8th Int. Fuzzy Syst. Assoc. World Congress, 1999, pp. 551–555.
[12] ISO/IEC 17799:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management, 2005, International Organization for Standardization, Geneva.
[13] ISO/IEC 27005:2011, Information Technology – Security Techniques – Information Security risk Management. 2005, International Organization for Standardization, Geneva.
[14] S. Kirkpatrick, C.D. Gelatt, M.P. Vecchi, Optimization by simulated annealing, Science 220 (1983) 671–680.
[15] H.S. Lee, An optimal aggregation method for fuzzy opinions of group decision, in: Proc. 1999 IEEE Int. Conf. Syst., Man. and Cybernetics, 1999, pp. 314–319.
[16] F. López Crespo, M.A. Amutio-Gómez, J. Candau, J.A. Mañas, Methodology for Information Systems Risk, Analysis and Management (MAGERIT version 2), Book I-The Method, Book II-Catalogue of Elements, Book III-The Techniques. Madrid: Ministerio de Administraciones Públicas, 2006a.
[17] Mehari 2010 – Risk Analysis and Treatment Guide, 2007, Club de la Sécurité de l'Information Francais (CSIF), Paris.
[18] A. Méndez Barco, J.A. Mañas, Manual del Usuario Pilar Basic versión 5.1, Centro Criptológico Nacional, Madrid, 2011.
[19] L. Peide, F. Jin, X. Zhang, Y. Su, M. Wang, Research on the multi-attribute decision-making under risk with interval probability based on prospect theory and the uncertain linguistic variables, Knowl.-Based Syst. 24 (2011) 554–561.
[20] J. Serrano-Guerrero, F.P. Romero, J.A. Olivas, Hiperion: a fuzzy approach for recommending educational activities based on the acquisition of competences, Inform. Sci. 248 (2013) 114–129.
[21] G. Stoneburner, A. Gougen, NIST 800-30 Risk Management, Guide for Information Technology Systems, National Institute of Standard and Technology, Gaithersburg, 2002.
[22] E. Vicente, A. Mateos, A. Jiménez, A new similarity function for generalized trapezoidal fuzzy numbers, artificial intelligence and soft computing, Lecture Notes Artificial Intelligence, vol. 7894, Springer, Berlin, 2013.
[23] E. Vicente, A. Mateos, A. Jiménez, Similarity functions for generalized trapezoidal fuzzy numbers: an improved comparative analysis, Comp. Math. Appl. (2013) (submitted for publication).
[24] E. Vicente, A. Jiménez, A. Mateos, A fuzzy extension on MAGERIT methodology for risk analysis in information systems, in: Proc. 6th IADIS Int. Conf. Inform. Syst., 2013, pp. 39–46.
[25] E. Vicente, A. Jiménez, A. Mateos, An interactive method of fuzzy probability elicitation in risk analysis, in: C. Huang, C. Karhaman (Eds.), Intelligent Systems and Decision Making for Risk Analysis and Crisis Response, CRC Press, 2013, pp. 223–228.
[26] W.P. Wang, Evaluating new product development performance by fuzzy linguistic computing, Expert Syst. Appl. 36 (2009) 9759–9766.
[27] J. Wang, J. Hao, A new version of 2-tuple fuzzy linguistic representation model for computing with words, IEEE Trans. Fuzzy Syst. 14 (2006) 435–445.
[28] S.H. Wei, S.M. Chen, A new approach for fuzzy risk analysis based on similarity measures of generalized fuzzy number, Expert Syst. Appl. 36 (2009) 589–598.
[29] G.-W. Wei, A method for multiple attribute group decision making based on the ET-WG and ET-OWG operators with 2-tuple linguistic information, Expert Syst. Appl. 37 (2010) 7895–7900.
[30] G.-W. Wei, X. Zhao, Some dependent aggregation operators with 2-tuple linguistic information and their application to multiple attribute group decision making, Expert Syst. Appl. 39 (2012) 5881–5886.
[31] Z.S. Xu, A method based on linguistic aggregation operators for group decision making with linguistic preference relations, Inform. Sci. 166 (2004) 19–30.
[32] Z.S. Xu, S. Shang, W. Qian, W. Shu, A method or fuzzy risk analysis based on the new similarity of trapezoidal fuzzy numbers, Expert Syst. Appl. 37 (2010) 1920–1927.
[33] L.A. Zadeh, Fuzzy sets, Inform. Control 8 (1965) 338–353.